A Novel Robust Spread Spectrum Watermarking Scheme for 3D Video Traitor Tracing

Karama Abdelhedi, Faten Chaabane, Faten Chaabane, William Puech, Chokri Ben Amar

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2023.0322000

A Novel Robust Spread Spectrum Watermarking Scheme for 3D Video Traitor Tracing

KARAMA ABDELHEDI[1], FATEN CHAABANE [1], (Member, IEEE), WILLIAM PUECH[2],(Senior Member, IEEE), and CHOKRI BEN AMAR [1], (Senior Member, IEEE)

[1]Research Groups in Intelligent Machines, ENIS, University of Sfax, Tunisia
[2]LIRMM, Université de Montpellier, CNRS 860 rue de St Priest, 34095 Montpellier, France

Corresponding author: Karama Abdelhedi (e-mail: karama.abdelhedi@enis.tn).

ABSTRACT The 3D video traitor tracing approach is an effective technique for securing 3D content. This approach involves the protection of the multimedia content and the prevention of each malicious manipulation by embedding the Collusion-Secure Fingerprinting (CSF) codes. Traitor tracing aims also at retrieving back the actors who contributed to the construction of an illegal release of a multimedia product by applying an efficient tracing scheme. Depending on the position of embedding the CSF codes, the current secure 3D video content schemes can be classified into three categories: the first one embeds the fingerprint into the 2D video, the second one into the depth maps' content, but each of these two categories protects only one component of the 3D video which gives rise to the proposal of a third category which embeds the fingerprint in both the two components of the 3D video and protects independently and simultaneously the 2D frames and the depth maps contents. This paper proposes a novel traitor tracing technique to protect the two essential components of 3D videos by embedding the CSF in the 2D frames and the depth maps by applying a novel and robust spread spectrum watermarking scheme. Experimental assessments demonstrate the effectiveness of this proposed technique by applying it to a case study of 3D games and show promising results in terms of speed and tracking accuracy constraints.

INDEX TERMS DIBR-based 3D video, Collusion-secure, Fingerprinting, Spread Spectrum, Traitors tracing, Tardos

I. INTRODUCTION

3D videos become more and more attractive and realistic than 2D videos. This type of visual media has highly expanded the user's interest and its popularity is essentially tied to video game applications. The 3D videos are of two major types according to their archiving format: the side by side videos format composed of the right and left views taken by two cameras with the same characteristics, and the Depth-Image-Based Rendering (DIBR) videos format, based on respectively 2D video frames and their corresponding depth maps. Most of the stored videos use the 3D-DIBR format because of its reduced storage size and transmission bandwidth costs compared to the first type. Due to the availability of the Internet and the huge evolution of the digital era, it becomes easy to modify, copy and re-distribute digital media. Unfortunately, digital video content can be prone to illegal manipulations, well-known as the digital piracy trials. Consequently, digital rights management (DRM) systems become crucial to control the use of digital content [1] and to protect any distributed media by preventing the illegal use of shared releases and detecting eventually malicious users. Traitor tracing as an effective technique for DRM involves the presence of both a fingerprinting technique and a tracing algorithm. The fingerprinting technique's role is to embed the fingerprint code which is assigned to a unique user in each release of the media to identify it and protect it from any illegal treatment. Then the tracing algorithm's objective is to retrieve malicious users. In this paper, we propose a robust fingerprinting scheme to protect DIBR-based 3D videos by protecting independently and simultaneously the copyright of their two major components: the 2D frames and the depth maps. The idea is to use a spread spectrum watermarking scheme to embed the identifier in both the 2D frames and the depth maps, then to implicate the suitable tracing technique to identify the illegal users in case of collusion attacks.

The paper is arranged as follows: Section II reviews the related work in multimedia tracing systems. Section III describes the spread spectrum watermarking scheme and Sec-

tion IV describes the tracing code, well-known as Tardos code. In Section V, we detail the different steps of the proposed tracing framework. In Section VI, we present the different experimental assessments we carry out to validate the performance of the proposed approach. Finally, we summarize with a conclusion and future work in Section VII.

II. RELATED WORK

Handling a great number of shared 3D videos and surviving different types of unauthorized manipulations present crucial challenges for the majority of fingerprinting schemes. In this context, several techniques were proposed in the literature. This section is divided into two sections. Section II-A focus on the watermarking techniques suitable for 3D videos while Section II-B is reserved for the tracing techniques.

A. OVERVIEW ON THE EXISTING 3D VIDEO WATERMARKING SCHEMES

Several watermarking schemes were suggested for DIBR-based videos [3]–[13]. Mainly, these schemes are divided into three classes according to the watermark embedding positions: 2D video frame-based watermarking, depth map-based watermarking and the third one is a hybrid scheme. Among the 2D video frame-based watermarking proposed schemes in the literature, a scheme proposed by [4] consists in constructing the Depth Perceptual Region of Interest (DP-ROI) by extracting some relevant characteristics such as gray contour regions, the foreground, and the depth-edge, to improve the embedding strength. Kim et al proposed a new watermarking scheme more robust against geometric distortion [5]. This scheme is based on the approximate shift invariance characteristics of a dual-tree complex wavelet to embed the watermark in the chrominance (U and V) channels. According to [6], the main weakness of 2D frames-based watermarking schemes is firstly tied to watermarking schemes that continue to treat 3D videos as conventional 2D videos and embed the watermark in the 2D frames and are not interested in protecting the copyright of the depth maps. So they do not satisfy the DRM requirements of DIBR-based 3D videos. Henceforth, the 2D frames-based watermarking schemes suffer from irreparable distortion to the synthesized 3D videos.

To cope with that issue, depth-map-based watermarking schemes were proposed. The particularity of this kind of approach is that watermarks are embedded into the depth maps, which guarantees that no distortions can be seen on the synthesized 3D videos [9]. A great deal of research has been carried out on depth-map schemes, ranging from the Unseen Visible (UVW) schemes [6]–[8]; where watermarks are embedded after estimating computations into the spatial domain by simply changing the pixel values of depth maps to enable easy and precise prior estimations. In the Unseen Extractable (UEW) schemes, the watermarks are hidden once DC quantization is performed. In both UVW-based schemes and UEW schemes, prior estimations are applied to restrict the modifications of depth maps. But those estimations limit the selection of watermark embedding methods and decrease the watermarking robustness. To address this issue, Liu et al [9] proposed an advanced unseen extractable watermarking(AUEW) scheme. This scheme used simulations of the embedding process rather than prior estimations to enhance the watermarking robustness. Similarly, it has been noticed by [11] that depth-map-based watermarking schemes do not respond to the requirements of DRM for DIBR-based 3D videos.

Consequently, the third family of watermarking schemes based on embedding watermarks in both 2D frames and depth maps was proposed. Among these techniques, zero-watermarking schemes were suggested where the watermark is not embedded in the signal host. The main steps of this type of watermarking scheme are the copyright registration step and its identification step [10]. In [11], the main contribution is to improve the traditional zero-watermarking schemes to be suitable for DIBR-based 3D videos. Although it proposed to protect both 2D frames and depth maps to ensure efficient robustness and good imperceptibility, its performance is reduced noticeably for high watermark bandwidth. In [12], a new SVM-based zero-watermarking technique for DIBR-based 3D videos is proposed, it has proven good results of robustness and transparency but it does not make any trace in the video copy which makes its tracing process harder. The work in [13] proposes a novel watermarking technique based on the LSB technique to protect the two components of the 3D video but this spacial domain technique is not robust enough against different kinds of attacks such as rotation and brightness.

To overcome this disadvantage, a novel robust spread spectrum (SS) watermarking scheme was proposed for 3D Video traitor tracing. Different from all other work, this scheme helps to protect simultaneously and independently the copyright of the 2d frames and the depth map. We distinguish, on the first side, the generation of the fingerprint by the Tardos code. Then This fingerprint is embedded in the two components of 3D video before diffusing the video copies to n users $U_{i\{1,\ldots,n\}}$. In the distributor side, a group of colluders colluder $j\{1..c\}$ mixes their copies and constructs a suspicious copy with an unknown fingerprint and diffused it. Once the suspicious copy is detected by the video supplier, the latter proceeds by extracting the colluded fingerprint and analyzing it to trace back the dishonest users.

B. THE TRACING TRAITOR: A BRIEF REVIEW

In the literature, several fingerprinting schemes have been proposed to improve collusion-secure codes to ameliorate their detection rates with fair lengths, even for a large number of users and pirates [21]. Massive research was investigated on the Tardos tracing process [18] which has proposed a good trade-off between the code length and the tracing rates [22]. In this context, several researchers focus on optimizing Tardos accusation's functions to ameliorate its robustness against the collusion attacks [24]–[31]. In other fingerprinting schemes, the target was to find a good trade-off between the tracing

code and the watermarking technique to provide a tracing scheme able to resist different types of collusion attacks [12], [13], [18]–[22]. But the robustness of these schemes was checked only against the averaging collusion attacks for a small number of users. In this paper, we propose a good trade-off between the adapted watermarking scheme and the Tardos-based tracing process that provides good tracing results for several collusion attacks. To our knowledge, we are the only ones proposing a tracing scheme for 3D videos and a use case for 3D video games.

III. SPREAD SPECTRUM WATERMARKING SCHEME

Initially, the spread spectrum was used to ensure the security of communication in the military domain. In the communication field, the spread spectrum system was defined by [42] as follows:

Spread spectrum is a mean of transmission in which the signal occupies a bandwidth in excess of the minimum necessary to send the information; the band spread is accomplished by a code which is independent of the data, and a synchronized reception with the code at the receiver is used for despreading and subsequent data recovery.

By analogy to the spread spectrum communications, Cox *et al.* [16] spread the watermark in the frequency domain by the Discrete Cosine Transforms (DCT), to protect the image. In cox *et al.* [16], *"the watermark is spread over many frequency bins to make the energy in any one very small and undetectable."* The DCT represents an image as a sum of sinusoids of varying magnitudes and frequencies. With an input image, X the coefficients for the output image X' is:

$$X'(z,y) = \sqrt{\tfrac{2}{M}}\sqrt{\tfrac{2}{N}}\alpha_z\alpha_y \sum_{i=0}^{M-1}\sum_{j=0}^{N-1} x(i,j)\cos\left[\tfrac{z\pi}{2M}(2i+1)\right]\cos\left[\tfrac{y\pi}{2N}(2j+1)\right], \tag{1}$$

where: $\alpha_i = \begin{cases} \frac{1}{\sqrt{2}}, & \text{for } i = 0 \\ 1, & \text{otherwise} \end{cases}$,

where N and M are the wide and high of the input image X, $X(i,j)$ is the intensity of the pixel in row m and column n, $X'(z,y)$ is the DCT coefficient in row z and column y of the DCT matrix.

The spread spectrum ensures then the embedding of a watermark $W = \{w_1, \cdots, w_n\}$ in a sequence of frequency $V = \{v_1, \cdots, v_n\}$ to obtain the sequence $V' = \{v'_1, \cdots, v'_n\}$ as follow: $v'_i = v_i + \alpha w_i$.

The spread spectrum hiding alleviated the weak points of the LSB technique. Certainly, the LSB ensures higher perceptual transparency but it is not very robust. Therefore the use of the spread spectrum provides excellent results in terms of perceptual transparency and robustness. Several robust watermarking techniques derived from this spread spectrum technique [40], [41] prove their robustness against many attacks like noise attacks, cropping, and geometrical attacks.

In another hand, spread spectrum hiding technique confirms the highly resistant to collusion attacks [41]. For this reason, [32] used the spread spectrum embedding technique to prevent any malicious collusion trial as shown in Fig. 1.

Consequently, [32] proposed a new derivation of the spread spectrum embedding method:

$$v'_j = v_j + \alpha U_k(-1)^{w(i,j)}, \tag{2}$$

with $w(i,j) = 0$ or 1 and U_k is a Gaussian sequence of size l. The attacked watermarked signal is $Z = Y + n$, where n is the noise due to the attack. The watermark bit $S'(i,j)$ is extracted from Z by the linear correlation of Z and U_k of length l as:

$$S'(i,j) = \begin{cases} 0, & if \sum_{j=0}^{l} Z[j]U_k[j] > 0 \\ 1, & if \sum_{j=0}^{l} Z[j]U_k[j] < 0 \end{cases} \tag{3}$$

IV. THE COLLUSION-SECURE FINGERPRINTING CODE: TARDOS CODE

We are interested in this work in the well-known (CSF) code, the Tardos code which was proposed by Gabor Tardos in 2003 [23]. This probabilistic binary code, compared to other existing codes, has provided a good compromise between code length and tracing results. The main idea of the Tardos code is to generate a $\{n \times m\}$ matrix X with n number of users and m the length of the codeword X_{ji} assigned to each user j, $i \in \{1...m\}$. The Tardos code model consists of three steps: initialization, construction and accusation.

- In the initialization step, a random and independent probability p_i was generated with the distribution $f(p) = \frac{1}{\pi\sqrt{p(1-p)}}$ for each codeword of length m. The length of the code is given as $m = \frac{1}{2}\pi^2 c^2 ln(\frac{1}{\varepsilon_1})$ with ε_1 and ε_2 respectively the false positive and false negative probabilities. we assume in this step that n, c, m and ε_1 and ε_2 are fixed with the condition: $1 < c$, $\varepsilon_1 < \varepsilon_2$. Practically $p_{i,\{1\le i\le m\}}$, $p_i \in \{0,1\}$ are chosen randomly and independently with: $t < p_i < 1-t$, t is a satisfying parameter, $t = \frac{1}{300c}$, $0 < t' < \frac{\pi}{4}$, $\sin^2 t' = t$, $p_i = sin^2 r_i$, with $r_i \in [t', \frac{\pi}{(2-t')}]$.
- The second step is the construction step. For n users, a $\{n \times m\}$ matrix X is constructed. And each element of X is generated independently with $Prob[X_{ji} = 1] = p_i$
- The last step is the accusation step. this step aims to determine if the user j participated in the creation of the suspicious code, an accusation score S_j in equ. (4) was calculated for each user j, $j \in \{1...n\}$ according to the symmetric accusation functions in equ. (5) and equ. (6) defined by [2] as follows:

$$S_j = \sum_{i=1}^{m} g\left(Y_i, X_{ji}, p_i\right), \tag{4}$$

$$g(1,1,p) = g(0,0,1-p) = \sqrt{\frac{(1-p)}{p}}, \tag{5}$$

$$g(1,0,p) = g(0,1,1-p) = -\sqrt{\frac{p}{(1-p)}}. \tag{6}$$

If $S_j > Z$, the output of the Tardos decoding algorithm includes a suspicious fingerprint j with a false positive

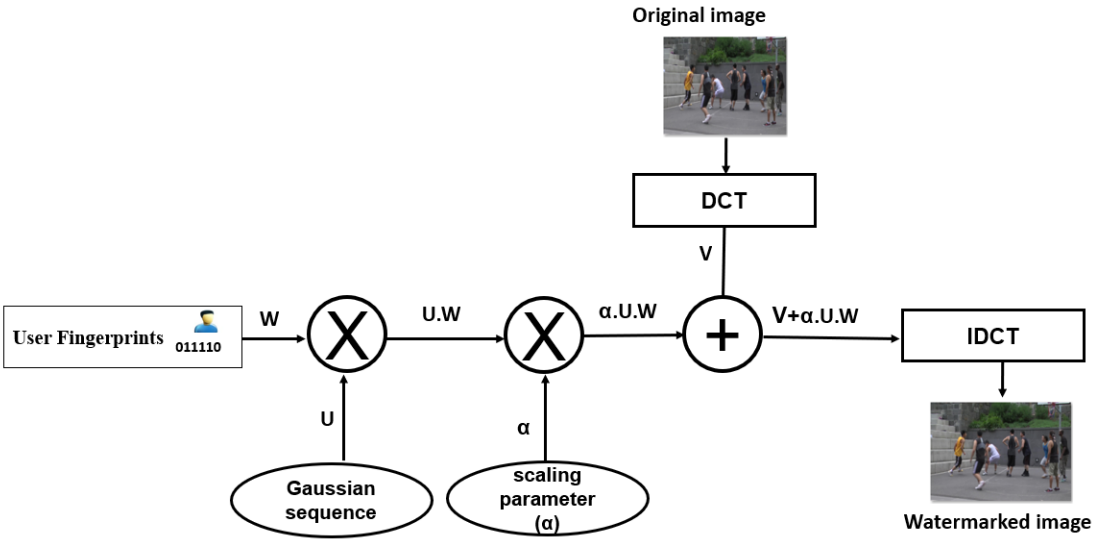

Figure 1: **The Spread Spectrum scheme.**

error $< \varepsilon_1$. Z is the threshold parameter [19] defined by:

$$Z = \pi c(\ln \frac{1}{\varepsilon_1}). \tag{7}$$

V. THE PROPOSED TRAITOR TRACING SCHEME FOR 3D VIDEOS

In [13], the traitor tracing system is defined as a system that aims to protect the delivered media in a distribution platform. The most important component in the tracing scheme is the fingerprinting code which identified each user. This system is based on three principal folds [13]:

- The copyrights registration phase: The purpose of this phase is to embed the fingerprinting code in the media by using a fingerprint embedding scheme that should respect the following requirements: imperceptibility, security, and robustness.
- Collusion attacks:In this phase, a group of dishonest users tries to generate and distribute new media copies. These illicit copies are produced by combining some of their copies.
- The copyrights identification phase: which target is to correctly extract the fingerprinting code from the suspicious release and then to provide the suspicious colluders.

According to

A. THE COPYRIGHT REGISTRATION PHASE

The new proposed Spread Spectrum Fingerprinting (SSF), is applied to the sequence of 2D frames and the sequence of depth maps frames simultaneously and independently. The proposed SSF starts with a preliminary step. The goal of this phase is to generate the user identification code and prepare the Groups Of Frames (GOF). The second step is the fingerprint embedding step in which the watermark is integrated into respectively GOFs of 2D and depth according to the spread spectrum technique. The detailed procedure of the proposed SSF is composed of two steps:

1) The preliminaries' step

Before the distribution of the copy of media, the media holder, assigns a unique fingerprint code-word, $I \in \{1, \cdots, m\}$ to each media release buyer. Moreover, the fingerprint or identifier should be unique and should identify the media owner to protect the digital content from any unauthorized treatment. In this context, we used the initialization and construction step of Tardos mentioned in section IV to generate the fingerprints' base.

To have a robust watermarking scheme we should increase the length of the fingerprinting code but at the same time, we should not decrease the quality of the image. The embedding of the watermark in each frame of the 2D frames or depth maps will may the distortions in synthesized 3D videos. Hence we should find a good conjunction to keep a robust watermarking scheme and conserve the high quality of the 3D video. So to resolve this problem we will divide the watermark into k parts and each part will be inserted in a frame. So to insert the totality of the watermark we need K frame. These K frames noted groups of frames (GOF). To optimize the result of the embedding phase, the sequences of both 2D frames and depth maps are divided into groups of frames (GOF). Each GOF is composed of k frames and is considered as a fingerprint carrier. In the case of N_f frames in the sequence, there are N_f/k groups.

The fingerprinting code will be embedded in each GOF of the sequence of 2D frames and of depth maps as depicted in Fig. 2.

To embed the fingerprinting code in a GOF, the code is also divided into k parts (P_w), and each part is embedded in one

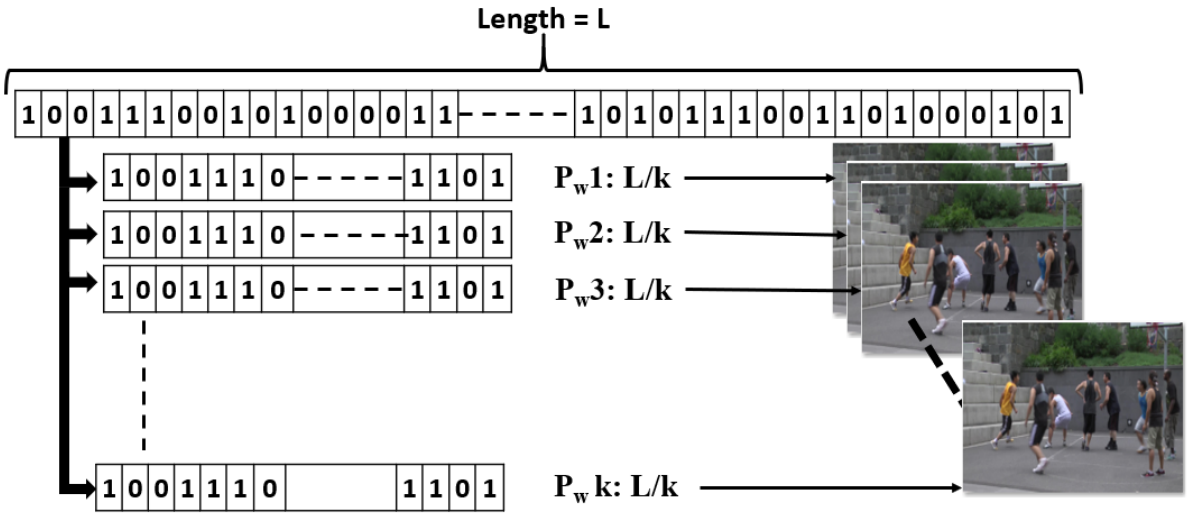

Figure 2: **The principle of GOF division.**

frame of the GOF. For an identifier code of length of L, we can generate k (P_w) with size L/k.

2) The fingerprint embedding step

In this phase, both of 2D frames and the depth sequences are protected simultaneously and independently by using a novel spread spectrum technique as shown in Fig. 3.

As depicted in Fig. 3, the copyright registration phase starts by dividing the sequence of frames into N_f/k GOF. Each GOF is composed of k frames. Then a fingerprint code of the owner user of the media copy is selected. This fingerprint is generated and saved in the user's database as mentioned in the preliminaries phase.

This step starts by converting the 2D frames from the RGB color space to YCbCr color space to separate the grayscale information from the color information. Then to avoid the problem of color distortion or alteration, the watermark sequence will be embedded in the luminance component Y. In the following, we will detail the process of the embedding technique which is applied to both 2D frames and depth maps.

The fingerprint is embedded in the different GOF of the same release in different positions. So the embedding position differed from frame to others and from video copies to others. In each frame will be inserted L/k bits of the fingerprint. To choose the position of the embedding, the Y component is divided into 8×8 blocks. Each block is converted in the frequency domain by applying the DCT. The blocks with the high band frequency of coefficients are selected to embed the fingerprint.

For the frame F_i, in the high band frequency of coefficients of the selected block, one bit of the fingerprint part (P_{wi}) is embedded by using the spread spectrum technique as explained in equ. (2) presented in Section III.

Finally, the fingerprint is embedded in all the GOF and the IDCT transformation is applied to generate the marked 2D frames and the marked depth maps. We detail the copyright registration phase with Algorithm 1.

Algorithm 1 Embedding fingerprinting algorithm

```
Divide the sequence of 2D frames in N_f/k GOF and the sequence of depth maps in N_f/k GOF
for j = 1 to N_f/k do
    for i = 1 to k do
        Divide the frame on blok of 8 × 8
        Apply the DCT to each block
        Select the corresponding part of the fingerprint P_wi
        Choose the block B which have the higher DCT
        choose pixel of higher DCT coefficient of the chosen bloc B to embed one bit of the fingerprint
        Apply the spread spectrum watermarking technique to embed the P_wi in the frame F_ji
        Apply the IDCT
    end for
end for
Generate the watermarked sequence of 2D frames and the watermarked sequence of depth maps
```

B. COLLUSION ATTACKS

To make the tracing phase more difficult, the colluders compare their different release and fixed a secret strategy to yield the suspicious fingerprint. This strategy is known as "the collusion attacks". In this section, we detail possible collusion attacks made under the Marking Assumption.

- The marking assumption:The Marking assumption was proposed in [14], it assumes that the colluders produce a suspicious copy after comparing their different releases. They will remark that in some positions their blocks are similar, and in this case, they will keep this block in the same positions on the pirated copy. But if the blocks are different, this signified that there is identifying informa-

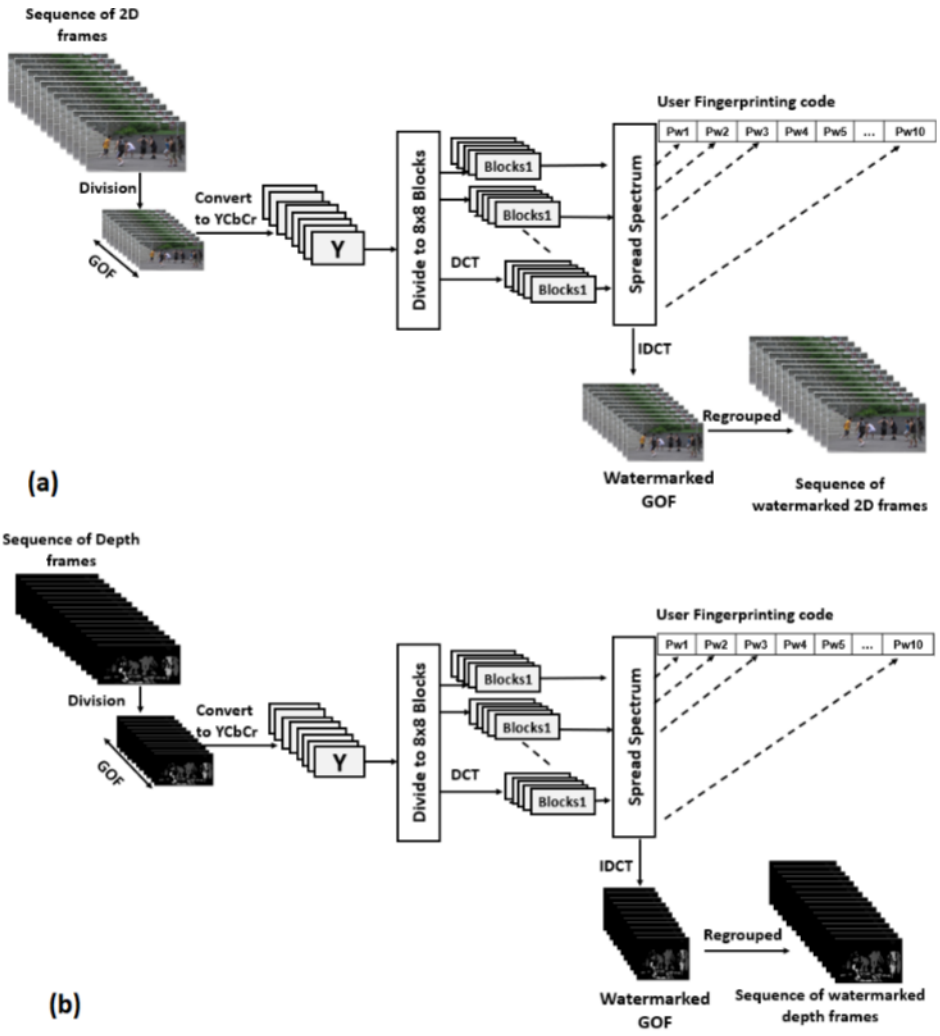

Figure 3: **The fingerprint embedding step: a) In the 2D video frames, b) In the depth maps.**

tion hidden in these blocks, so they will modify in some way these hidden symbols.

According to [15], the attacks can be classified in three categories:

- The Block exchange attack: In this type of scenario, the symbol in the suspicious copy can be one of the symbols of colluders' codewords for a position. There are several strategies integrated into this type such as the majority/minority vote attacks, All-one, All-zero.
- Fusion attack: In this case of attack, the pirates combine their respective blocks to compute the block in the suspicious copy with one strategy: average, minimum, maximum, median, etc.
- Individual signal processing: The suspicious copy is altered with post-processing made by colluders to erase the way to trace them. This treatment can be, a compression, noising, denoising, or filtering.

In following, we detail the different collusion attacks we apply in our experimentation. Suppose that malicious users collude to produce a pirated copy $y = \{y_1, ..., y_l\}$ using their copies $x_j = \{x_{j1}, ..., x_{jl}\}$. Some typical examples of collusion attacks are given as follows:

$$Average: y_t^{avg} = \frac{1}{v}\sum_{j=1}^{v} x_{jt} \tag{8}$$

$$\text{Majority: } y_t^{maj} = \begin{cases} 0, if \sum_{j=1}^{v}(x_{jt} = 0) > v/2 \\ 1, if \sum_{j=1}^{v}(x_{jt} = 1) > v/2 \end{cases} \tag{9}$$

$$All\_one: y_t^{All\_one} = \begin{cases} 0, if \sum_{j=1}^{v}(x_{jt} = 0) > 1 \\ 1, if \sum_{j=1}^{v}(x_{jt} = 1) = v \end{cases} \tag{10}$$

$$All\_zero: y_t^{All\_zero} = \begin{cases} 1, if \sum_{j=1}^{v}(x_{jt} = 1) > 1 \\ 0, if \sum_{j=1}^{v}(x_{jt} = 0) = v \end{cases} \tag{11}$$

C. THE COPYRIGHT IDENTIFICATION PHASE

Once the distribution of the watermarked video is done, the media can be the target of many malicious treatments and attacks. The most important one is the collusion one which has as its purpose to hide the identity of the video owner. For this reason, the main objective of the copyright identification phase is to determine whose colluder participates in the creation of the illegal version of the video.

1) The fingerprint extracting step

The goal of the fingerprint-extracting step is to detect the embedded fingerprint from the suspicious video by using the appropriate watermark extraction process. This extraction process is the reverse process of the watermark embedding process. This phase takes as input a sequence of 2D frames and a sequence of depth maps of fingerprinted 3D video to return as output the extracted fingerprint code $W' = \{w'_1, w'_2, \cdots, w'_m\}$ as depicted in Fig. 4.

Algorithm 2 resumes the fingerprint extracting step.

2) The Tracing technique

In the case of the extracted code, the fingerprint extraction step is classed by the supplier as an unknown fingerprint. We use the tracing technique to trace back colluders. The tracing process is based on the Tardos code which was presented in Section IV.

Algorithm 2 Extract fingerprinting algorithm

1: Divide the sequence of 2D frames in N_f/k GOF and the sequence of depth maps in N_f/k GOF.
2: **for** $j = 1$ to N_f/k **do**
   % extract the fingerprint codes from 2D sequence
3: **for** $i = 1$ to k **do**
4: Apply the 2D_DCT.
5: Choose the block B which have the higher DCT.
6: Choose pixel of higher DCT coefficient of the chosen block B to extract one bit of the fingerprint.
7: Extract from F_{ji} part of the fingerprint $P_{w'_j} = \{w'1, \cdots, w'n\}$ by using the spread spectrum technique.
8: Apply the D_IDCT.
9: **end for**
10: Regrouped the different part of the fingerprint $W'_j = \{w'1, \cdots, w'm\}$.
11: **end for**
12: Repeat the steps from 2 to 9 to extract the fingerprint codes from the depth maps sequence.
13: Apply the majority vote technique (MVT) to the extracted fingerprint to determine the final detected fingerprint code.

VI. EXPERIMENTAL RESULTS

In this section, we evaluate firstly the robustness of the proposed SSF scheme. Then, we evaluate the efficiency of its tracing process against different collusion attacks. The tested database contains 150 different 3D video clips collected from the database [38]. Other 2D video clips are selected from different movies, with their corresponding depth maps calibrated using the technique in [39]. Each video of the database contains respectively 100 2D frames and 100 of depth maps of size 1920×1080. And the sequence of 2D frames and depth maps is divided into different GOF consisting of $k = 10$ frames.

A. THE WATERMARKING RESULTS

In this section, we evaluate the proposed scheme's robustness and imperceptibility.

1) Imperceptibility results:

To demonstrate the watermarking scheme's efficiency, it is important to evaluate its imperceptibility. In this context, we compute the Peak signal to noise ratio (PSNR):

$$PSNR = 10 \log \frac{255^2}{\frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} (I(i,j) - I'(i,j))^2}. \quad (12)$$

Table 1 presents the different PSNR values depending on the watermark length embedded in the 3D video. The high rates of PSNR show that the proposed scheme guarantees an efficient imperceptibility of the embedded watermarks.

Table 1: PSNR VALUES.

Fingerprint length (bits)		2450	6810	15330
PSNR (dB)	2D frames	49.8	47.7	45.6
	Depth maps	43.8	43.6	43.3

2) Robustness to signal processing attacks

We compute the Normalized Correlations (NC) criterion and the Bit Correction Rate (BCR) between the original and recovered watermarks to assess the robustness of the proposed approach against collusion attempts.

$$NC_{2d} = \frac{\sum W_{2d}(i) W'_{2d}(i)}{\sqrt{\sum W_{2d}(i)^2} \sqrt{\sum W'_{2d}(i)^2}}, \quad (13)$$

$$BCR(W, W') = 1 - \frac{1}{2} \sum_{k=1}^{n} \left| W_k - W'_k \right|, \quad (14)$$

where $1 \leq i \leq L$ *and* $1 \leq k \leq L$.

In Table 2 we compare the NC and BCR values in three case—using only 2D frames, using only depth maps, and in the case of our proposed scheme— with the same fingerprinting length $L = 6810$ and different attacks. It is observed that the proposed scheme is the most robust against the different attacks.

The higher NC and BCR values indicate stronger watermarking robustness.

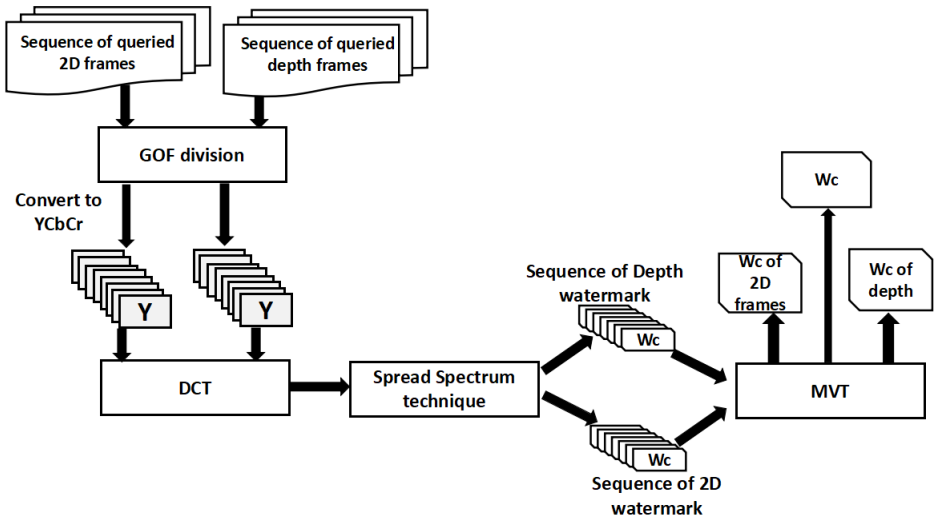

Figure 4: **Copyright identification phase.**

Table 2: NC AND BCR VALUES.

Attack	Only using 2D frames		Only using depth maps		Proposed	
	NC	BCR	NC	BCR	NC	BCR
Average filtering 3	1	0.99	0.76	0.63	1	1
Average filtering 5	0.99	0.92	0.76	0.63	0.99	0.99
Average filtering 9	0.73	0.72	0.71	0.6	0.88	0.89
Median filtering 3	1	0.99	0.76	0.63	1	1
Median filtering 5	0.99	0.92	0.76	0.63	0.99	0.99
Median filtering 9	0.73	0.72	0.71	0.6	0.93	0.93
Gaussian noise (0.01)	1	0.92	0.86	0.6	0.99	0.99
Gaussian noise (0.03)	0.99	0.83	0.93	0.7	0.99	0.99
Gaussian noise (0.05)	0.96	0.76	0.8	0.7	0.96	0.96
Salt & pepper (0.005)	0.99	0.99	0.97	0.97	0.99	0.99
Salt & pepper (0.01)	0.98	0.98	0.74	0.69	0.97	0.97
Salt & pepper (0.03)	0.93	0.93	0.64	0.6	0.75	0.78
resize (1/2)	1	0.98	0.82	0.62	1	1
resize (1/4)	0.76	0.75	0.71	0.6	0.96	0.96
brightness (+30%)	1	1	0.82	0.76	1	1
brightness (-30%)	1	1	0.82	0.76	1	1
Cropping	1	1	0.82	0.76	1	1

Table 3: Compare NC VALUES.

Attack	[13]		Proposed technique	
	2D frames	Depth maps	2D frames	Depth maps
Average filtering 9	0.6	0.48	0.73	0.71
Gaussian noise (0.05)	0.95	0.87	0.96	0.8
Salt & pepper (0.01)	0.98	0.99	0.98	0.74
Salt & pepper (0.03)	0.96	0.97	0.93	0.64
resize (1/4)	0.6	0.48	0.76	0.71
brightness (+30%)	0.5	0.5	1	0.82
brightness (-30%)	0.5	0.5	1	0.82

3) Comparison to other audio watermarking techniques

In this part, we try to compare our watermarking technique to [13] the only work that embedded the watermark in both components of 3D videos. In Table 3 we compare the Nc value when we used the watermarking technique proposed by [13] and when we used our proposed watermarking technique.

B. THE TRACING RESULTS

In this section, we test the robustness of the tracing technique against some collusion attacks. In Fig 5 we give an illustration example for each tested collusion attack.

In order to prove the performance of the proposed system in terms of tracing rates, we take respectively the number of users to $n = 50$, the false positive probability to $\epsilon_1 = 10^{-6}$, the size of the fingerprint embedded in the video is $L = 6810$, and the number of the colluded users is respectively $2, 4, 6, 8$, and 10.

The experimental results, which are shown in Fig. 6, demonstrate our system's effective and accurate tracing performance against attacks such as Majority vote, Average, All-one, and All-zero. Without any wrongly accused users, we can find all colluders using majority vote and average attacks, but with all-one and all-zero assaults, we can only detect about half of the colluders.

C. CASE STUDY: 3D VIDEO GAMES

For this section, we pulled a video clip from YouTube for the video game "Apex Legends". From this 3D sequence, we retrieve the 2D frames and their Depth Maps.

1) The watermarking results:

This section examines the robustness of the video game's watermarking technique. Hence in the first phase, we contrasted the original image with the watermarked image and the targeted image (Average filtering 5, Brightness, Gaussian noise (0.05), Median filtering 9) As shown in Fig. 7. The NC and BCR values are then calculated in three scenarios—using only 2D frames, using only depth maps, and in the case of our proposed scheme—to confirm the method's robustness as indicated in Table 4

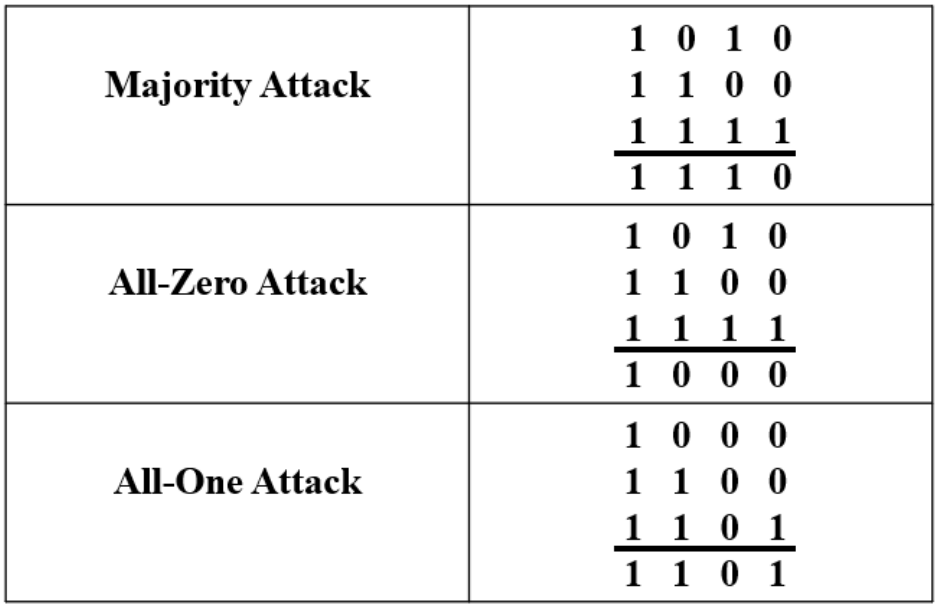

Figure 5: **Exemples for tested collusion attacks.**

Table 4: NC AND BCR VALUES.

Attack	Only using 2D frames		Only using depth maps		Proposed	
	NC	BCR	NC	BCR	NC	BCR
Average filtering 3	1	0.99	0.5	0.5	0.7	0.74
Average filtering 5	0.99	0.96	0.5	0.5	0.7	0.74
Median filtering 3	1	0.98	0.71	0.7	1	1
Median filtering 5	0.98	0.83	0.7	0.6	0.98	0.98
Median filtering 9	0.87	0.7	0.7	0.6	0.86	0.86
Gaussian noise (0.01)	0.94	0.84	0.5	0.5	0.67	0.72
Gaussian noise (0.03)	0.76	0.69	0.5	0.5	0.6	0.64
Salt & pepper (0.005)	1	0.98	0.82	0.74	1	1
Salt & pepper (0.01)	1	0.97	0.81	0.73	1	1
Salt & pepper (0.03)	0.99	0.93	0.82	0.72	1	1
Salt & pepper (0.05)	0.98	0.87	0.8	0.7	0.97	0.97
brightness (+30%)	1	1	0.81	0.74	1	1
brightness (-30%)	1	1	0.82	0.76	1	1
Cropping	1	1	0.82	0.75	1	1

2) The tracing results

The purpose of this section is to assess how well the tracing approach works. So, we demonstrate the outcome of the test of the collusion attacks in the video game in Fig. 8. In this test, the number of users is $n = 50$ and the size of the fingerprint is $L = 6810$. In the case of Majority and Average attacks, all the colluders have been successfully traced. But in the case of All_one and All_zero attacks, we detect same wrongly accused users.

VII. CONCLUSIONS AND FUTURE WORK

The 3D video traitor tracing technique is a promising method for securing 3D content by protecting multimedia content and preventing malicious manipulation. The paper proposed a novel traitor tracing technique that embeds the collusion-secure fingerprint in both the 2D frames and depth maps, providing independent and simultaneous protection of both components of the 3D video. The use of a spread spectrum watermarking technique was found to be effective in experimental assessments of 3D games, with promising results in terms of rapidity and tracking accuracy constraints.

Overall, this paper demonstrates the importance of developing new techniques for securing 3D content, particularly in the face of increasing digital piracy and unauthorized distribution. The proposed traitor tracing technique has the potential to improve the security of 3D video content, and further research in this area could lead to new and innovative ways to protect multimedia content in the future.

References

[1] M.D. de Rosnay, Digital rights management systems and European law: between copyright protection and access control, Second International Conference on Web Delivering of Music, pp.117-124, 2002.

[2] B. Škorić, S. Katzenbeisser and M. Celik, Symmetric Tardos Fingerprinting Codes for Arbitrary Alphabet Sizes,Des. Codes Cryptography,vol.46 pp.137–166,2008.

[3] M. Lee, J. Lee, and H. Lee, Perceptual Watermarking for 3D Stereoscopic Video Using Depth Information, Seventh International Conference on Intelligent Information Hiding and Multimedia Signal Processing, pp.81-84, 2011.

[4] F. Sheng-Li, Y. Mei, J. Gang-Yi, S. Feng, P. Zong-Ju and F. Sheng-li, A Digital Watermarking Algorithm Based on Region of Interest for 3D Image, 2012 Eighth International Conference on Computational Intelligence and Security, pp.549-552, 2012.

[5] H. Kim, J. Lee, T. Oh and H. Lee, Robust DT-CWT Watermarking for DIBR 3D Images,58, IEEE Transactions on Broadcasting, pp.533-543,2012.

[6] Y. Lin and J. Wu, Unseen visible watermarking for color plus depth map 3D images, 2012 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pp.1801-1804,2012.

[7] S. Pei and Y. Wang, Auxiliary Metadata Delivery in View Synthesis Using Depth No Synthesis Error Model, 17, IEEE Transactions on Multimedia,pp.128-133,2015.

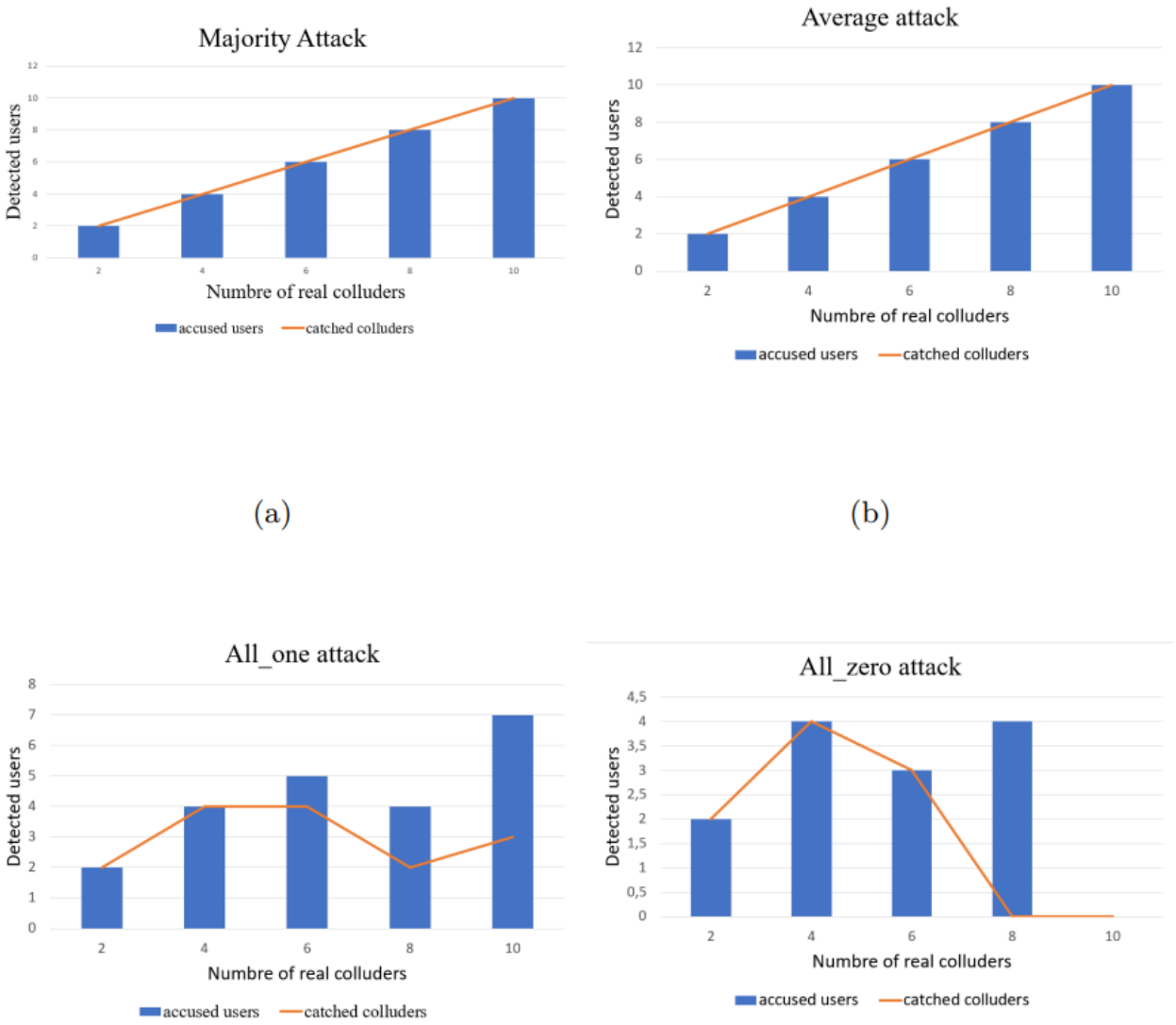

Figure 6: **Tracing performance against some attacks.**

[8] S.-C. Pei, Y.-Y. Wang, A new 3D unseen visible watermarking and its applications to multimedia, 2014 IEEE 3rd Global Conference on Consumer Electronics, GCCE, pp.140-143,2015.
[9] X. Liu, F. Li, J. Du, Y. Guan, Y. Zhu, B. Zou, A robust and synthesized-unseen watermarking for the DRM of DIBR-based 3D video, Neurocomputing. ,pp.155-169,2017
[10] G. Guangyong and J. Guoping, Bessel-Fourier moment-based robust image zero-watermarking, 74,Multimedia Tools and Applications,pp.841-858, 2015
[11] X. Liu R. Zhao , L. Fangfang , S. Liao , D.Yipeng, Z. Beiji , Novel robust zero-watermarking scheme for digital rights management of 3D videos,Signal Processing: Image Communication, vol.54, pp.140 - 151, 2017.
[12] K. Abdelhedi, F. Chaabane and C. Ben Amar, A SVM-Based Zero-Watermarking Technique for 3D Videos Traitor Tracing, Advanced Concepts for Intelligent Vision Systems, pp.373-383,2020.
[13] K. Abdelhedi, F. Chaabane, W. Puech and C. Ben Amar, Toward a Novel LSB-based Collusion-Secure Fingerprinting Schema for 3D Video, Computer Analysis of Images and Patterns, pp.58-68,2021.
[14] D. Boneh , j. Shaw, Collusion-secure fingerprinting for digital data. IEEE Trans Inf Theory, pp.1897–1905,1998.
[15] W. Trappe, Z. Jane Wang, K. J. Ray Liu, Anti-collusion fingerprinting for multimedia, IEEE Transactions on Signal Processing pp.1069–1087, 2003.
[16] I.J. Cox, J. Kilian , F.T. Leighton and T. Shamoon, Secure spread spectrum watermarking for multimedia, IEEE transactions on image Processing, vol.6, pp.1673-1687,1997.
[17] F. Chaabane, M. Charfeddine, W. Puech, and C. Ben Amar, A two-stage traitor tracing scheme for hierarchical fingerprints,76,Multimedia Tools and Applications,pp.14405-14435,2017.
[18] G. Tardos, Optimal Probabilistic Fingerprint Codes, 2008.
[19] T. Laarhoven,and B. de Weger, Optimal symmetric Tardos traitor tracing schemes, Designs Codes and Cryptography, vol.71, pp.83-103,2014.
[20] V.K. Sharma, and V. Shrivastava, A steganography algorithm for hiding image in image by improved LSB substitution by Minimize detection,36 Journal of Theoretical and Applied Information Technology, pp.1-8, 2012.
[21] S. He and M. Wu, Collusion-Resistant Video Fingerprinting for Large User Group, IEEE Transactions on Information Forensics and Security, pp.697-709, 2007.
[22] C. Peikert , A. Shelat and A. Smith, Lower Bounds for Collusion-Secure Fingerprinting, pp.472-479, 2003.
[23] G. Tardos, Optimal Probabilistic Fingerprint Codes, Journal of the ACM,2004.

(a) Initiale image

(b) Watermarked image

(c) Average attack

(d) Brigtness attack

(e) Gaussian attack

(f) Median attack

Figure 7: Same attacks:a) Initial image, b) Watermarked image, c) Average filtering 5, d) Brightness, e) Gaussian noise (0.05), f) Median filtering 9x9.

[24] M. Desoubeaux, G. Le Guelvouit and W. Puech, Fast detection of Tardos codes withboneh-shaw types 8303,Media Watermarking, Security, and Forensics, SPIE, 2012 url = http://www.rmit3dv.com.

[25] F. Chaabane, M. Charfeddine , W. Puech and C. Ben Amar, A QR-code based audio watermarking technique for tracing traitors, 23rd European Signal Processing Conference (EUSIPCO), pp.51-55,2015.

[26] F. Chaabane, M. Charfeddine, W. Puech and C. Ben Amar, Towards a Blind MAP-Based Traitor Tracing Scheme for Hierarchical Fingerprints, Neural Information Processing, pp.505-512,2015.

[27] S. Craver, N. Memon, B. Yeo and M.M. Yeung, Resolving rightful ownerships with invisible watermarking techniques: limitations, attacks, and implications, pp.573-586,1998.

[28] M. Elárbi, C. Ben Amar and H. Nicolas , Video Watermarking Based on Neural Networks, 2006 IEEE International Conference on Multimedia and Expo, pp.1577-1580, 2006.

[29] M. Fernandez, M. Soriano and J. Cotrina, Tracing illegal redistribution using errors-anderasures and side information decoding algorithms,Information Security,IET,,pp.83-90,2007.

[30] T. Furon and L. Pérez-Freire, Worst case attacks against binary probabilistic traitor tracing codes, 2009 First IEEE International Workshop on Information Forensics and Security (WIFS),pp.56-60,2009.

[31] F. Chaabane, M. Charfeddine and C. Ben Amar, An Enhanced Hierarchical Traitor Tracing Scheme Based on Clustering Algorithms, pp.379-390,2017.

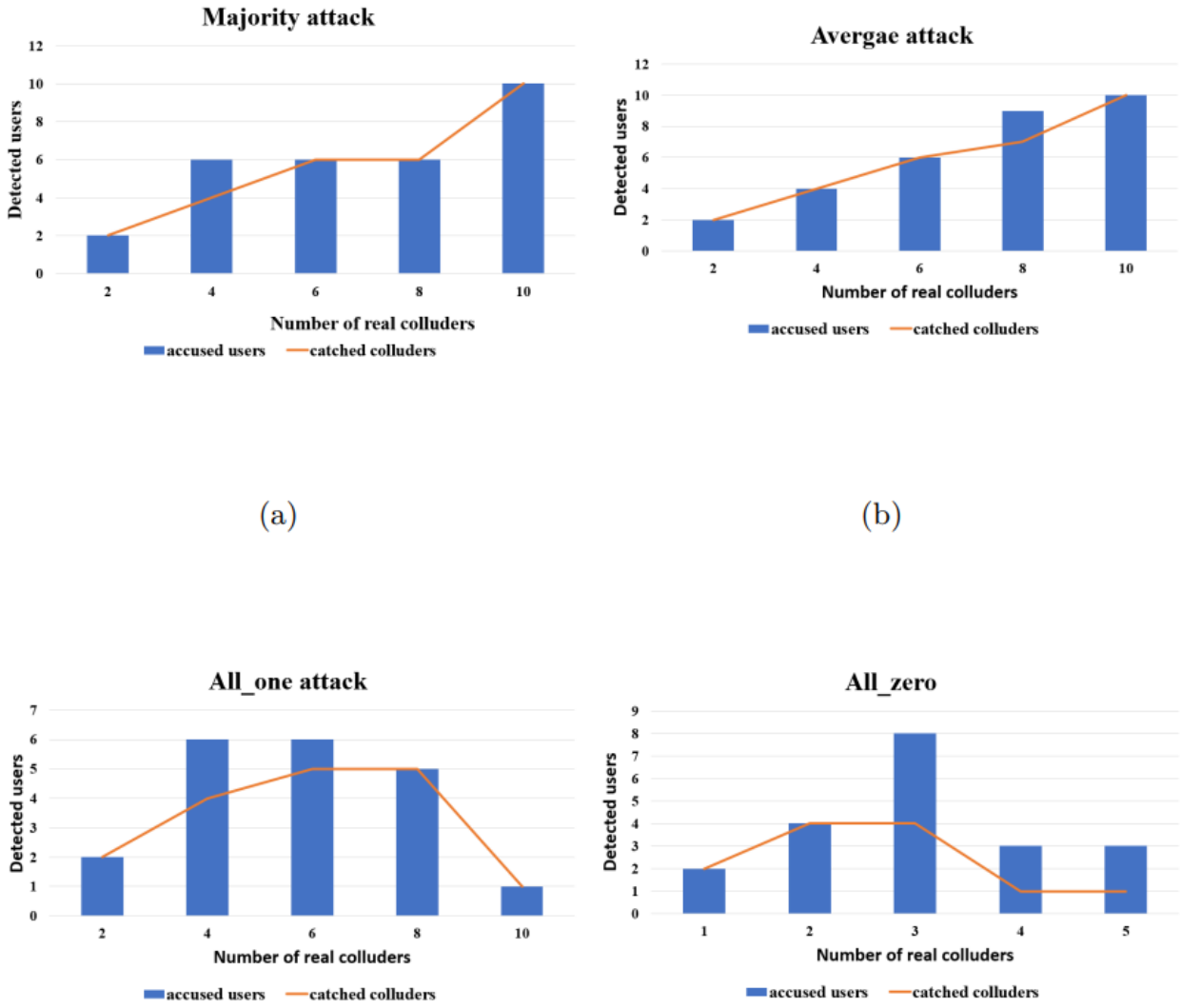

Figure 8: **Collusion attacks applicated to the video games.**

[32] Z. Shahid, M. Chaumont and W. Puech, 2010 IEEE International Conference on Image Processing,Spread spectrum-based watermarking for Tardos code-based fingerprinting for H.264/AVC video, pp.2105-2108, 2010, doi=10.1109/ICIP.2010.5652607

[33] N. Hayashi, M. Kuribayashi and M. Masakatu, Advances in Information and Computer Security, Collusion-Resistant Fingerprinting Scheme Based on the CDMA-Technique,978-3-540-75651-4, Springer Berlin Heidelberg,Berlin, Heidelberg,pp.28–43,2007.

[34] M. Koubaa,C. Ben Amar and H. Nicolas, Collusion-Resistant Video Watermarking Based on Video Mosaicing, Eighth IEEE International Symposium on Multimedia (ISM06),pp.161-168,2006.

[35] F. Chaabane , M. Charfeddine and C. Ben Amar, A survey on digital tracing traitors schemes, 2013 9th International Conference on Information Assurance and Security ,IAS, pp.85-90, 2013.

[36] M. Desoubeaux , G. Le Guelvouit and W. Puech, Probabilistic fingerprinting codes used to detect traitor zero-bit watermark, Media Watermarking, Security, and Forensics III, pp.334-342, 2011.

[37] B. Appina, S.V.R. Dendi, K. Manasa , S.S. Channappayya and A.C. Bovik, Study of Subjective Quality and Objective Blind Quality Prediction of Stereoscopic Videos, IEEE Transactions on Image Processing,2019.

[38] E. Cheng , P. Burton , J. Burton, A. Joseski and I. Burnett, RMIT3DV: Pre-announcement of a creative commons uncompressed HD 3D video database, 2012 Fourth International Workshop on Quality of Multimedia Experience, pp.212-217,2012.

[39] D. Scharstein, R. Szeliski, and R. Zabih, A taxonomy and evaluation of dense two-frame stereo correspondence algorithms, Proceedings IEEE Workshop on Stereo and Multi-Baseline Vision (SMBV 2001), pp.131-140, 2001.

[40] F. Hartung, Su. Jonathan and B. Girod, Spread Spectrum Watermarking: Malicious Attacks and Counterattacks, Security and Watermarking of Multimedia Contents, 2000.

[41] J.Ò. Ruanaidh and T. Pun, Rotation, scale and translation invariant spread spectrum digital image watermarking, Signal Process,vol.66, pp.303-317,1998.

[42] R. Pickholtz, D. Schilling, and L. Milstein, Theory of Spread-Spectrum Communications - A Tutorial, IEEE Transactions on Communications, vol. 30, pp. 855-884,1982.

KARAMA ABDELHEDI graduated from the Higher Institute of Computer Science and Multimedia of Sfax (ISIMS) in 2011, received the Master's degree in Computer Science and Multimedia from the Higher Institute of Computer Science and Multimedia of Sfax (ISIMS) in 2013. She is currently progressing the Phd degree in the National Engineering School of Sfax. Nowadays, she is member of the Research Group of Intelligent Machine (REGIM Laboratory) as Phd student . Her research interests include digital tracing traitor and video watermarking.

FATEN CHAABANE Faten Chaabane graduated from the National School of Engineers of Sfax in 2006, obtained her Master's degree in Communication Systems from the National School of Engineers of Tunis in 2012 and her Ph.D in Computer Systems Engineering in March 2017. Currently, she is an Associate Professor in the Department of Computer Science and Multimedia at ISLAIB Beja, University of Jendouba. Her research work mainly focuses on cybersecurity, watermarking, multimedia document tracing, and since 2020, she has been interested in securing data with Blockchain architectures.

WILLIAM PUECH received the diploma of Electrical Engineering from the Univ. Montpellier, France (1991) and a Ph.D. Degree in Signal-Image-Speech from the Polytechnic National Institute of Grenoble, France (1997) with research activities in image processing and computer vision. He served as a Visiting Research Associate to the University of Thessaloniki, Greece. From 1997 to 2008, he has been an Associate Professor at the Univ. Montpellier, France. Since 2009, he is a full Professor in image processing at the Univ. Montpellier, France. His current interests are in the areas of image forensics and security for safe transfer, storage and visualization by combining data hiding, compression, cryptography and machine learning. He is head of the ICAR team (Image and Interaction) in the LIRMM and has published more than 50 journal papers and 160 conference papers and is associate editor for 4 journals (SPIC, SP, JVCIR and IEEE TDSC) in the areas of image forensics and security and senior area editor for IEEE TIFS. Since 2017 he has been the general chair of the IEEE Signal Processing French Chapter. He has been a member of the IEEE Information Forensics and Security TC between 2018 and 2020 and then again since 2022. Since 2021 he has also been member of the IEEE Image, Video and Multidimensional Signal Processing TC.

CHOKRI BEN AMAR received the B.S. degree in Electrical Engineering from the National Engineering School of Sfax (ENIS) in 1989, the M.S. and PhD degrees in Computer Engineering from the National Institute of Applied Sciences in Lyon, France, in 1990 and 1994, respectively. He spent one year at the University of "Haute Savoie" (France) as a teaching assistant and researcher before joining the higher School of Sciences and Techniques of Tunis (ESSTT) as Assistant Professor in 1995. In 1999, he joined the Sfax University (USS) as Assistant Professor, and since 2011 as a full professor in the Department of Computer Sciences and Applied Mathematics of the National Engineering School of Sfax. Since September 2018, he is a full professor at the college of Computers and Information technology of Taif University in Saudi Arabia. His research interests include Computer Vision and Image and video analysis. These research activities are centered on intelligent algorithms and their applications to data Classification and approximation, Pattern Recognition, Watermarking and image and video indexing and securing. He is a senior member of IEEE since 2008. He founded the IEEE Signal Processing Society (SPS) Tunisia Chapter on January 2009, and he is actually the chair of this Chapter. During this period, the chapter organized five IEEE Distinguished Lectures and other technical and professional activities. He is the current advisor of the IEEE SPS Student Chapter in ENIS since 2010.